CHAPTER 41

ソフトウェア、ライセンス、およびコンフィギュレーションの管理

この章では、セキュリティ アプライアンスのソフトウェア、ライセンス、およびコンフィギュレーションの管理について説明します。この章では、次の項目について説明します。

ライセンスの管理

ソフトウェアをインストールすると、元のイメージから既存のアクティベーション キーが抽出され、セキュリティ アプライアンス ファイル システムのファイル内に保存されます。

アクティベーション キーの取得

アクティベーション キーを取得するには、シスコの代理店から購入できる Product Authorization Key が必要になります。Product Authorization Key を入手したら Web 上でキーを登録し、次の手順を実行してアクティベーション キーを取得します。

ステップ 1　次のコマンドを入力して、セキュリティ アプライアンスのシリアル番号を取得します。

```
hostname> show version | include Number
```

パイプ文字（|）をコマンドの一部として入力します。

ステップ 2　Web ブラウザを次のいずれかの Web サイトに接続します（URL は大文字と小文字を区別します）。

Cisco.com の登録ユーザの場合は、次の Web サイトを使用します。

```
http://www.cisco.com/go/license
```

Cisco.com の登録ユーザ以外の場合は、次の Web サイトを使用します。

```
http://www.cisco.com/go/license/public
```

ステップ 3　プロンプトが表示されたら、次の情報を入力します。

- Product Authorization Key
- セキュリティ アプライアンスのシリアル番号
- 電子メール アドレス

アクティベーション キーが自動的に生成され、指定した電子メール アドレスに送信されます。

新しいアクティベーション キーの入力

アクティベーション キーを入力するには、次のコマンドを入力します。

```
hostname(config)# activation-key key
```

キーは、4 つまたは 5 つのエレメントからなる 16 進文字列です。各エレメントは 1 つのスペースで区切られます。たとえば、正しい形式のキーは次のようになります。

0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e

先頭部分の 0x 指定子は省略できます。値は、すべて 16 進数であると見なされます。

すでにマルチコンテキスト モードに入っている場合は、システム実行スペースにこのコマンドを入力します。

アクティベーション キーを入力する前に、フラッシュ メモリ内のイメージと実行イメージが同一であることを確認します。これは、セキュリティ アプライアンスをリブートしてからアクティベーション キーを入力することで確認できます。

（注）　アクティベーション キーは、コンフィギュレーション ファイルには保存されません。キーはデバイスのシリアル番号に結び付けられます。

実行イメージで変更内容を有効にするには、新しいアクティベーション キーを入力した後でセキュリティ アプライアンスをリブートする必要があります。

次の例は、セキュリティ アプライアンスでアクティベーション キーを変更する方法を示しています。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

フラッシュ メモリ内のファイルの表示

フラッシュ メモリ内のファイルを表示して、そのファイルに関する情報を確認できます。

- フラッシュ メモリ内のファイルを表示するには、次のコマンドを入力します。

  ```
  hostname# dir [flash: | disk0: | disk1:]
  ```

  flash: キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:** または **disk0:** を使用できます。**disk1:** キーワードは、ASA の外部フラッシュ メモリを表します。内部フラッシュ メモリがデフォルトです。

  次の例を参考にしてください。

  ```
  hostname# dir

  Directory of disk0:/
  500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
  2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
  2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
  2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
  ```

- 特定のファイルに関する拡張情報を表示するには、次のコマンドを入力します。

  ```
  hostname# show file information [path:/]filename
  ```

  デフォルト パスは、内部フラッシュ メモリ（flash:/ または disk0:/）のルート ディレクトリです。

  次の例を参考にしてください。

  ```
   show file information cdisk.bin

  disk0:/cdisk.bin:
    type is image (XXX) []
    file size is 4976640 bytes version 7.0(1)
  ```

  示されているファイル サイズは例にすぎません。

フラッシュ メモリへのソフトウェアまたはコンフィギュレーションのダウンロード

アプリケーション イメージ、ASDM イメージ、コンフィギュレーション ファイル、および他のファイルを TFTP、FTP、HTTP、または HTTPS サーバから内部フラッシュ メモリに、あるいは ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合は外部フラッシュ メモリに、ダウンロードできます。

ここでは、次の項目について説明します。

特定の場所へのファイルのダウンロード

この項では、アプリケーション イメージ、ASDM ソフトウェア、コンフィギュレーション ファイル、またはフラッシュ メモリへのダウンロードが必要な他のファイルのダウンロード方法について説明します。ファイルを実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにダウンロードする場合は、P.41-5 の「スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード」を参照してください。

Cisco SSL VPN クライアントのインストールの詳細については、P.38-2 の「SVC ソフトウェアのインストール」を参照してください。セキュリティ アプライアンスへの Cisco Secure Desktop のインストールについては、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

複数のイメージがインストールされている場合、または外部フラッシュ メモリにイメージがインストールされている場合に特定のアプリケーション イメージまたは ASDM イメージを使用するようにセキュリティ アプライアンスを設定する場合は、P.41-6 の「ブートするアプリケーション イメージと ASDM イメージの設定」を参照してください。

（注）　ASDM バージョン 5.0(5) をフラッシュ メモリにコピーするには、バージョン 7.0 を実行する必要があります。

特定のコンフィギュレーションをスタートアップ コンフィギュレーションとして使用するようにセキュリティ アプライアンスを設定する場合は、P.41-7 の「スタートアップ コンフィギュレーションとしてブートするファイルの設定」を参照してください。

マルチコンテキスト モードの場合は、システム実行スペース内にいる必要があります。

ファイルをフラッシュ メモリにダウンロードするには、各ダウンロード サーバ タイプ用の次のコマンドを参照してください。

- TFTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy tftp://server[/path]/filename {flash:/ | disk0:/ |
  disk1:/}[path/]filename
  ```

  flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:/** または **disk0:/** を使用できます。**disk1:/** キーワードは、ASA の外部フラッシュ メモリを表します。

- FTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename {flash:/ | disk0:/ | disk1:/}[path/]filename
  ```

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename {flash:/ | disk0:/ | disk1:/}[path/]filename
  ```

- セキュア コピーを使用するには、まず SSH をイネーブルにしてから、次のコマンドを入力します。

  ```
  hostname# ssh scopy enable
  ```

  その後、Linux クライアントから次のコマンドを入力します。

  ```
  scp -v -pw password filename username@fwsm_address
  ```

  -v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード

TFTP、FTP、または HTTP(S) サーバから、またはフラッシュ メモリから、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにテキスト ファイルをダウンロードできます。

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションにファイルをコピーするには、適切なダウンロード サーバに対して次のコマンドのいずれかを入力します。

（注） コンフィギュレーションを実行コンフィギュレーションにコピーするには、2　つのコンフィギュレーションをマージします。マージは、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドを追加します。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

- TFTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy tftp://server[/path]/filename {startup-config | running-config}
  ```

- FTP サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename {startup-config | running-config}
  ```

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename
  {startup-config | running-config}
  ```

- フラッシュ メモリからコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {flash:/ | disk0:/ | disk1:/}[path/]filename
  {startup-config | running-config}
  ```

たとえば、TFTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy http://209.165.200.228/configs/startup.cfg startup-config
```

ブートするアプリケーション イメージと ASDM イメージの設定

デフォルトでは、セキュリティ アプライアンスは内部フラッシュ メモリ内で見つけた最初のアプリケーション イメージをブートします。また、内部フラッシュ メモリ内で見つけた最初の ASDM イメージをブートするか、内部フラッシュ メモリ内にない場合は外部フラッシュ メモリ内の ASDM イメージをブートします。複数のイメージがある場合は、ブートするイメージを指定する必要があります。ASDM イメージの場合は、ブートするイメージを指定しないと、インストールされているイメージが 1 つしかなくても、セキュリティ アプライアンスは **asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Update（設定されている場合）の問題を避けるため、また起動時ごとのイメージ検索を回避するため、ブートする ASDM イメージをスタートアップ コンフィギュレーションで指定する必要があります。

- ブートするアプリケーション イメージを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# boot system url
  ```

  ここで、*url* は次のいずれかです。

  - {**flash:/** | **disk0:/** | **disk1:/**}[*path*/]*filename*

    flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:/** または **disk0:/** を使用できます。**disk1:/** キーワードは、ASA の外部フラッシュ メモリを表します。

  - **tftp://**[*user*[**:***password*]**@**]*server*[*:port*]/[*path*/]*filename*

    このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみサポートされています。

  最大 4 つの **boot system** コマンド エントリを入力して、ブートする別々のイメージを順番に指定することができます。セキュリティ アプライアンスは、最初に見つけたイメージをブートします。設定できる **boot system tftp:** コマンドは 1 つだけです。これは、最初に設定する必要があります。

- ブートする ASDM イメージを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# asdm image {flash:/ | disk0:/ | disk1:/}[path/]filename
  ```

スタートアップ コンフィギュレーションとしてブートするファイルの設定

デフォルトでは、セキュリティ アプライアンスは、隠しファイルであるスタートアップ コンフィギュレーションからブートします。あるいは、次のコマンドを入力して、任意のコンフィギュレーションをスタートアップ コンフィギュレーションとして設定することもできます。

```
hostname(config)# boot config {flash:/ | disk0:/ | disk1:/}[path/]filename
```

flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:/** または **disk0:/** を使用できます。**disk1:/** キーワードは、ASA の外部フラッシュ メモリを表します。

フェールオーバー ペアのゼロ ダウンタイム アップグレードの実行

フェールオーバー コンフィギュレーション内の 2 つの装置は、同一のメジャー（最初の番号）およびマイナー（2 番目の番号）ソフトウェア バージョンを持っている必要があります。ただし、アップグレード処理中に装置のバージョン パリティを維持する必要はなく、各装置でそれぞれ異なるバージョンのソフトウェアを実行しても、フェールオーバー サポートを維持することができます。互換性と安定性を長期間確保するためには、両装置をできるだけ早期に同じバージョンにアップグレードすることをお勧めします。

表 41-1 に、フェールオーバー ペアのゼロダウンタイム アップグレードの例を示します。

表 41-1　ゼロダウンタイム アップグレード サポート

アップグレードの種類	サポートの内容
メンテナンス リリース	任意のメンテナンス リリースから、マイナー リリースの範囲で他のメンテナンス リリースにアップグレードできます。 たとえば、7.0(1) から 7.0(4) の範囲であれば、最初にメンテナンス リリースをインストールしなくてもアップグレードが可能です。
マイナー リリース	マイナー リリースから次のマイナー リリースにアップグレードできます。途中のマイナー リリースをスキップしてアップグレードすることはできません。 たとえば、7.0 からは 7.1 にアップグレードできます。ゼロダウンタイム アップグレードでは 7.0 から 7.2 への直接のアップグレードはサポートされていません。まず 7.1 にアップグレードする必要があります。
メジャー リリース	直前のバージョンの最終マイナー リリースから次のメジャー リリースにアップグレードできます。 たとえば、7.x リリースにおける最終のマイナー バージョンが 7.9 であると想定される場合、7.9 から 8.0 にアップグレードできます。

フェールオーバー ペアのソフトウェアのアップグレードについて詳しくは、次の項目を参照してください。

- Active/Standby フェールオーバー コンフィギュレーションのアップグレード（P.41-8）
- Active/Active フェールオーバー コンフィギュレーションのアップグレード（P.41-9）

Active/Standby フェールオーバー コンフィギュレーションのアップグレード

Active/Standby フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

ステップ 1　両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを **boot system** コマンド（P.41-6 の「ブートするアプリケーション イメージと ASDM イメージの設定」を参照）で指定します。

ステップ 2　アクティブ装置に次のコマンドを入力して、スタンバイ装置をリロードして新規イメージをブートします。

```
active# failover reload-standby
```

ステップ 3　スタンバイ装置がリロードを終了し、Standby Ready 状態になったら、アクティブ装置で次のコマンドを入力して、アクティブ装置をスタンバイ装置に強制的にフェールオーバーします。

（注）　**show failover** コマンドを使用して、スタンバイ装置が Standby Ready 状態にあることを確認します。

```
active# no failover active
```

ステップ 4　次のコマンドを入力して、前のアクティブ装置（現在の新規スタンバイ装置）をリロードします。

```
newstandby# reload
```

ステップ 5　新規スタンバイ装置がリロードを終了し、この装置が Standby Ready 状態になったら、次のコマンドを入力して元のアクティブ装置をアクティブな状態に戻します。

```
newstandby# failover active
```

Active/Active フェールオーバー コンフィギュレーションのアップグレード

Active/Active フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

ステップ 1　両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを **boot system** コマンド（P.41-6 の「ブートするアプリケーション イメージと ASDM イメージの設定」を参照）で指定します。

ステップ 2　プライマリ装置のシステム実行スペースで次のコマンドを入力して、プライマリ装置の両方のフェールオーバー グループをアクティブにします。

```
primary# failover active
```

ステップ 3　プライマリ装置のシステム実行スペースで次のコマンドを入力して、セカンダリ装置をリロードして新規イメージをブートします。

```
primary# failover reload-standby
```

ステップ 4　セカンダリ装置のリロードが終了し、その装置で両方のフェールオーバー　グループが　Standby Ready 状態になったら、プライマリ装置のシステム実行スペースで次のコマンドを実行して、セカンダリ装置で両方のフェールオーバー グループをアクティブにします。

（注）　**show failover** コマンドを使用して、両方のフェールオーバー グループがセカンダリ装置で Standby Ready 状態にあることを確認します。

```
primary# no failover active
```

ステップ 5　両方のフェールオーバー グループがプライマリ装置で Standby Ready 状態にあることを確認してから、次のコマンドを使用してプライマリ装置をリロードします。

```
primary# reload
```

ステップ 6　フェールオーバー グループが **preempt** コマンドで設定されている場合は、これらはプリエンプション遅延の経過後、指定された装置で自動的にアクティブになります。フェールオーバー グループを **preempt** コマンドで設定していない場合、**failover active group** コマンドを使用すると、これらのグループを指定された装置でアクティブな状態に戻すことができます。

コンフィギュレーション ファイルのバックアップ

コンフィギュレーションをバックアップするには、次のいずれかの方法で行います。

シングルモード コンフィギュレーションまたはマルチモードのシステム コンフィギュレーションのバックアップ

シングルコンテキスト モードで、またはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバまたはローカルのフラッシュ メモリにコピーできます。

- TFTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config} tftp://server[/path]/filename
  ```

- FTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config}
  ftp://[user[:password]@]server[/path]/filename
  ```

- ローカルのフラッシュ メモリにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {startup-config | running-config} {flash:/ | disk0:/ |
  disk1:/}[path/]filename
  ```

  宛先のディレクトリが存在することを確認してください。存在しない場合は、最初に、**mkdir** コマンドを使用してディレクトリを作成します。

コンテキスト コンフィギュレーションのフラッシュ メモリへのバックアップ

マルチコンテキスト モードで、システム実行スペースで次のコマンドのいずれかを入力して、ローカルのフラッシュ メモリにあるコンテキスト コンフィギュレーションをコピーします。

- TFTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy disk:[path/]filename tftp://server[/path]/filename
  ```

- FTP サーバにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy disk:[path/]filename ftp://[user[:password]@]server[/path]/filename
  ```

- ローカルのフラッシュ メモリにコピーするには、次のコマンドを入力します。

  ```
  hostname# copy {flash:/ | disk0:/ | disk1:/}[path/]filename {flash:/ | disk0:/ |
  disk1:/}[path/]newfilename
  ```

  宛先のディレクトリが存在することを確認してください。存在しない場合は、最初に、**mkdir** コマンドを使用してディレクトリを作成します。

コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ

マルチコンテキスト モードでは、コンテキスト内から次のバックアップを実行できます。

- （admin コンテキストに接続された）スタートアップ コンフィギュレーション サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

  ```
  hostname/contexta# copy running-config startup-config
  ```

- コンテキスト ネットワークに接続された TFTP サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

  ```
  hostname/contexta# copy running-config tftp:/server[/path]/filename
  ```

端末の表示からのコンフィギュレーションのコピー

コンフィギュレーションを端末に表示するには、次のコマンドを入力します。

```
hostname# show running-config
```

このコマンドの出力内容をコピーし、テキスト ファイルにコンフィギュレーションを貼り付けます。

Auto Update サポートの設定

Auto Update は、Auto Update Server がコンフィギュレーションとソフトウェア イメージを多数のセキュリティ アプライアンスにダウンロードすることを許可し、中央からのセキュリティ アプライアンスの基本的なモニタリングを提供するプロトコル仕様です。

セキュリティ アプライアンスは、クライアントまたはサーバとして設定できます。Auto Update クライアントとして設定すると、Auto Update Server を定期的にポーリングして、ソフトウェアのイメージとコンフィギュレーション ファイルのアップデートを要求します。Auto Update Server として設定すると、Auto Update クライアントとして設定されているセキュリティ アプライアンス用のアップデートを発行します。

（注）　Auto Update は、シングルコンテキスト モードでのみサポートされます。

ここでは、次の項目について説明します。

- Auto Update Server との通信の設定（P.41-13）
- Auto Update Server としてのクライアント アップデートの設定（P.41-15）
- Auto Update ステータスの表示（P.41-16）

Auto Update Server との通信の設定

セキュリティ アプライアンスを Auto Update クライアントとして設定するには、次の手順に実行します。

ステップ 1　AUS の URL を指定するには、次のコマンドを使用します。

```
hostname(config)# auto-update server url [source interface] [verify-certificate]
```

ここで、*url* には次のシンタックスがあります。

```
http[s]://[user:password@]server_ip[:port]/pathname
```

https を指定すると、SSL が使用されます。URL の *user* 引数と *password* 引数は、サーバにログインするときの基本認証に使用されます。**write terminal**、**show configuration**、または **show tech-support** コマンドを使用してコンフィギュレーションを表示した場合、ユーザとパスワードは「********」に置換されます。

HTTP のデフォルト ポートは 80、HTTPS のデフォルト ポートは 443 です。

source *interface* 引数は、AUS に要求を送信するときに使用するインターフェイスを指定します。**management-access** コマンドで指定したインターフェイスと同じインターフェイスを指定すると、Auto Update 要求は管理アクセスに使用されるのと同じ IPSec VPN トンネルを通過します。

verify-certificate キーワードは、AUS によって戻される証明書を確認します。

ステップ 2　（オプション）AUS と通信する際に送信するデバイス ID を識別するには、次のコマンドを入力します。

```
hostname(config)# auto-update device-id {hardware-serial | hostname | ipaddress
[if-name] | mac-address [if-name] | string text}
```

使用する ID は、次のいずれかのパラメータによって決まります。

- **hardware-serial**：セキュリティ アプライアンスのシリアル番号を使用します。
- **hostname**：セキュリティ アプライアンスのホスト名を使用します。
- **ipaddress**：指定したインターフェイスの IP アドレスを使用します。インターフェイス名を指定しない場合、AUS との通信に使用するインターフェイスの IP アドレスを使用します。
- **mac-address**：指定したインターフェイスの MAC アドレスを使用します。インターフェイス名を指定しない場合、AUS との通信に使用するインターフェイスの MAC アドレスを使用します。
- **string**：指定されたテキスト識別子を使用します。空白や ‘、“、、>、&、? は使用できません。

ステップ 3　（オプション）コンフィギュレーション、またはイメージの更新を要求するために AUS がポーリングする回数を指定するには、次のコマンドを入力します。

```
hostname(config)# auto-update poll-period poll-period [retry-count [retry-period]]
```

poll-period 引数は、更新を確認する間隔（分単位）を指定します。デフォルトは 720 分（12 時間）です。

retry-count 引数は、サーバへの最初の接続に失敗した場合に、再試行する回数を指定します。デフォルトは 0 です。

retry-period 引数は、リトライの間の待機時間（分単位）を指定します。デフォルトは 5 です。

ステップ 4　（オプション）セキュリティ アプライアンスで Auto Update Server をポーリングする特定の時間を設定するには、次のコマンドを使用します。

```
hostname(config)# auto-update poll-at days-of-the-week time [randomize minutes] [retry_count
[retry_period]]
```

days-of-the-week には、曜日（Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、Sunday）を 1 つまたは組み合せて指定します。この他にも、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、weekend（土曜日と日曜日）を指定できます。

time には、ポーリングを開始する時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時を、20:00 は午後 8 時を示します。

randomize *minutes* は、指定した開始時刻以降に、ポーリング時間をランダム化する期間を指定します。ポーリングする期間は 1 ～ 1439 分の範囲で指定できます。

retry_count は、Auto Update Server に接続できなかったときに、再試行回数を指定します。デフォルトは 0 です。

retry_period は、再試行する間隔を指定します。デフォルトは 5 分です。1 ～ 35791 分の値を指定できます。

ステップ 5　（オプション）Auto Update Server に一定期間アクセスがなかった場合にトラフィックの通過を中断するには、次のコマンドを使用します。

```
hostname(config)# auto-update timeout period
```

ここで、*period* は 1 ～ 35791 の分単位のタイムアウト期間を指定します。デフォルトはタイムアウトなし（0）です。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスに最新のイメージとコンフィギュレーションがあることを確認するには、このコマンドを使用します。この状態は、システム ログ メッセージ 201008 で報告されます。

次の例では、セキュリティ アプライアンスが外部インターフェイスから証明書の検証付きで、IP アドレス 209.165.200.224、ポート番号 1742 で AUS をポーリングするように設定されています。

さらに、セキュリティ アプライアンスのホスト名としてデバイス ID を使用し、毎週金曜日と土曜日の午後 10 時から 11 時の間、任意にポーリングし、接続できなかった場合は AUS で 3 分間隔で 10 回再試行するように設定しています。

```
hostname(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside
verify-certificate
hostname(config)# auto-update device-id hostname
hostname(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
```

Auto Update Server としてのクライアント アップデートの設定

client-update コマンドを使用すると、Auto Update クライアントとして設定されているセキュリティ アプライアンスをアップデートできます。アップデートするソフトウェア コンポーネントのタイプ（ADSM またはブート イメージ）、セキュリティ アプライアンスのファミリ、リビジョン番号、およびアップデートの取得先の URL か IP アドレスを指定します。

セキュリティ アプライアンスを Auto Update Server として設定するには、次の手順を実行します。

ステップ 1　グローバル コンフィギュレーション モードで、コマンドを入力してクライアント アップデートをイネーブルにします。

```
hostname(config)# client-update enable
hostname(config)#
```

ステップ 2　**client-update** コマンドを使用して、セキュリティ アプライアンスに適用するクライアント アップデートのパラメータを設定します。

client-update {**component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} ***url*** *url-string* ***rev-nums*** *rev-nums*}

component {**asdm** | **image**} では、ソフトウェア コンポーネント（ASDM またはセキュリティ アプライアンスのブート イメージ）を指定します。

device-id *dev_string* では、アップデートする Auto Update クライアント自体を示す固有の文字列を指定します。最大長は 63 文字です。

family *family_name* では、アップデートする Auto Update クライアント自体の固有のファミリ名を指定します。asa、pix、または 7 文字以内のテキスト文字列を指定します。

rev-nums *rev-nums* では、このクライアントのソフトウェアまたはファームウェア イメージを指定します。任意の順番で 4 つまで、カンマで区切って指定できます。

type *type* では、アップデートを知らせるクライアントのタイプを指定します。このコマンドは、Windows クライアントのアップデートにも使われるので、Windows オペレーティング システムもいくつか指定できます。セキュリティ アプライアンスのタイプは次のとおりです。

- pix-515：Cisco PIX 515 Firewall
- pix-515e：Cisco PIX 515E Firewall
- pix-525：Cisco PIX 525 Firewall
- pix-535：Cisco PIX 535 Firewall
- asa5505：Cisco 5505 適応型セキュリティ アプライアンス

- asa5510：Cisco 5510 適応型セキュリティ アプライアンス
- asa5520：Cisco 5520 適応型セキュリティ アプライアンス
- asa5540：Cisco 適応型セキュリティ アプライアンス

***url** url-string* で、ソフトウェアまたはファームウェアのイメージの URL を指定します。必ず、このクライアントに適したファイルのある URL を指定してください。どの Auto Update クライアントでも、URL のプレフィックスとして http:// または https:// プロトコルを使用する必要があります。

特定のタイプのすべてのセキュリティ アプライアンスに適用するクライアント アップデートのパラメータを設定します。つまり、セキュリティ アプライアンスのタイプ、およびアップデートされたイメージの取得先の URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。リモートのセキュリティ アプライアンスのリビジョン番号が、指定したものと同じ場合はアップデートする必要がありません。クライアントは、アップデートを無視します。

次の例は、Cisco 5500 適応型セキュリティ アプライアンスのクライアント アップデートを設定しています。

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

Auto Update ステータスの表示

Auto Update のステータスを表示するには、次のコマンドを入力します。

```
hostname(config)# show auto-update
```

次に、**show auto-update** コマンドの出力例を示します。

```
hostname(config)# show auto-update
Server: https://********@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```